IN THE CLAIMS:

Please amend the claims as follows:

1. (Currently Amended) A method for the generation of forgery-proof documents or data records, whereby key information is generated and whereby encrypted checking information is formed from the key information and from a transaction indicator,

comprising: ~~the steps of~~

generating key information in a contact station;

forming encrypted checking information from the key information and from the transaction indicator in the contact station,

encrypting the key information in the contact station,

transmitting the encrypted checking information and the encrypted key information to an intermediate station,

storing the encrypted key information and the encrypted checking information in the intermediate station and subsequently transmitting the encrypted key information and the encrypted checking information to a cryptographic module at a different time from the transfer between the contact station and the intermediate station,

decrypting the encrypted key information with a key contained in the cryptographic module,

irreversibly linking document data to the key information,

combining the document data and the key information that is irreversibly linked to the document data to form at least one of a document and a data record, and

transmitting the document or data record to a checking station.

2. (Previously Presented) The method according to Claim 1, comprising randomly generating the key information.

3. (Previously Presented) The method according to Claim 1, comprising configuring at least one of the encrypted key information and the encrypted checking information in such a way that it cannot be decrypted in the intermediate station.

4. (Canceled)

5. (Currently Amended) The method according to Claim 1, comprising entering the document data into the cryptographic module.

6. (Canceled)

7. (Currently Amended) The method according to Claim [[6]] 1, comprising irreversibly linking the document data and the key information by forming a check value from the key information.

8. (Canceled)

9. (Currently Amended) The method according to Claim [[8]] 1, wherein the document or data record transmitted to the checking station is transmitted at least partially in plain text.

10. (Currently Amended) The method according to Claim [[8]] 1, comprising entering the encrypted checking information into the document or data record that is transmitted to the checking station.

11. (Previously Presented) The method according to Claim 1, comprising encrypting information remaining in the cryptographic module in such a way that it can be decrypted in the cryptographic module.

12. (Previously Presented) The method according to Claim 11, comprising supplying the cryptographic module with the information from a cryptographically reliable station that can be relied on by the checking station.

13. (Previously Presented) The method according to Claim 12, comprising using cryptographic encryptions that the checking station can reverse.

14. (Previously Presented) The method according to Claim 12, comprising supplying the cryptographic module via communication partners that are cryptographically non-reliable and forwarding information to the cryptographic module at a different point in time from the transfer of information between the contact station and the intermediate station.

15. (Previously Presented) The method according to Claim 12, comprising supplying the cryptographic module via communication partners that are cryptographically not reliable in such a way that an exchange of information within a dialog is not necessary.

16. (Previously Presented) The method according to Claim 1, comprising cryptographically linking the key information and the encrypted checking information to each other, such that said linking cannot be discovered by means of crypto-analysis.

17. (Previously Presented) The method according to Claim 16, wherein the cryptographic linking of the key information and the encrypted checking information is such that non-linear fractions are added that are known only to the reliable contact station and to the checking station.

18. (Previously Presented) The method according to Claim 1, wherein the generated forgery-proof documents or data records contain monetary value information.

19. (Previously Presented) The method according to Claim 18, comprising cryptographically connecting the monetary value information to the document or data record, and forming a check value by comparing the monetary value information to the document or data record.

20. (Previously Presented) The method according to Claim 18, wherein the monetary value information contains proof of the payment of postage amounts.

21. (Previously Presented) The method according to Claim 20, comprising linking the monetary value information to identification data.

22. (Previously Presented) The method according to Claim 20, comprising linking the monetary value information to address data.

23. (Currently Amended) A system comprising a value transfer center with an interface for loading monetary values and a cryptographic module, wherein the value transfer center comprises: ~~comprising~~

an interface to receive encrypted checking information and encrypted key information from a cryptographically reliable contact station and to temporarily store the encrypted information and encrypted key information;

a means of receiving value transfer requests from at least one cryptographic module; and

a means of forwarding the received encrypted checking information and encrypted key information to the cryptographic module at a different point in time from a transfer of information between the cryptographically reliable contact station and the interface,

and wherein the cryptographic module comprises:

at least one means for receiving and decrypting the key information;

at least one means for receiving a document or data record; and

at least one means for forming a check value for the document or for the data record using the key information.

24. (Currently Amended) The ~~value transfer center~~ system according to Claim 23, wherein the checking information and the key information are ~~is~~ encrypted in such a way that ~~it~~ the checking information and the key information cannot be decrypted in the value transfer center.